PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification: **H04Q 7/38, H04L 9/08**	**A1**	(11) International Publication Number:	**WO 00/56105**
		(43) International Publication Date:	21 September 2000 (21.09.2000)

(21) International Application Number: PCT/FI00/00223

(22) International Filing Date: 17 March 2000 (17.03.2000)

(30) Priority Data:
990601 17 March 1999 (17.03.1999) FI

(60) Parent Application or Grant
SONERA SMARTTRUST OY [/]; (). VATANEN, Harri [/]; (). VATANEN, Harri [/]; (). PAPULA OY ; ().

Published

(54) Title: ARRANGEMENT FOR SECURE COMMUNICATION AND KEY DISTRIBUTION IN A TELECOMMUNICATION SYSTEM

(54) Titre: PROCEDE ET SYSTEME DANS UN SYSTEME DE TELECOMMUNICATIONSN IN A TELECOMMUNICATION SYSTEM

(57) Abstract

The present invention relates to telecommunication systems. The object of the invention is to disclose a method and system for secure routing of information and addressing of a service and the parties to the service in a telecommunication system comprising a telecommunication terminal (1); a telecommunication network (2); a service provider (SP) connected to the telecommunication network (2); a service apparatus (4 connected to the telecommunication network (2); and a communication link (5) provided between the telecommunication terminal (1) and the service apparatus (4). In the method, the service apparatus (4) and/or the service mediated by it as well as the telecommunication terminal (1) are provided with an unambiguous identifier associated with predetermined encryption and/or signing keys. Further, a given service apparatus (4) is addressed by means of the telecommunication terminal (1) by sensing a predetermined connection setup request from the telecommunication terminal (1) to the given service apparatus (4). Further, the service provider's (SP) network address and/or other information relating to the selected service is sent from the telecommunication terminal (1) to the service apparatus (4) via the communication link (5). The communication link is preferably based on Bluetooth technology.

(57) Abrégé

La présente invention concerne des systèmes de télécommunication et en particulier un procédé et un système permettant l'acheminement sûr d'informations et l'accès à un service et aux parties concernées par ce service dans un système de télécommunications qui comporte un terminal (1) de télécommunications, un réseau (2) de télécommunications, un fournisseur de services (SP) connecté au réseau (2) de télécommunications, un appareil (4) de service connecté au réseau (2) de télécommunications et une liaison (5) de communication reliant le terminal (1) de télécommunications et l'appareil (4) de services. Selon ledit procédé, l'appareil (4) de service et/ou le service fourni par son intermédiaire ainsi que le terminal (1) de télécommunications sont dotés d'un identificateur non ambigu associé à des clés prédéterminées de codage et/ou de signature. En outre, le terminal (1) de télécommunications s'adresse à un appareil (4) donné de services en envoyant une demande d'établissement de connexion prédéterminée à cet appareil (4) de services. De plus, l'adresse de réseau du fournisseur de services (SP) et/ou d'autres informations relatives au service choisi sont envoyées depuis le terminal (1) de télécommunications à l'appareil (4) de services via la liaison (5) de communication. La liaison de communication est de préférence basée sur la technologie sans fil _ Bluetooth _.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04Q 7/38, H04L 9/08

A1

(11) International Publication Number: **WO 00/56105**

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/FI00/00223

(22) International Filing Date: 17 March 2000 (17.03.00)

(30) Priority Data:
990601 17 March 1999 (17.03.99) FI

(71) Applicant *(for all designated States except US)*: SONERA SMARTTRUST OY [FI/FI]; c/o Sonera Oyj, P.O. Box 106, FIN-00051 Sonera (FI).

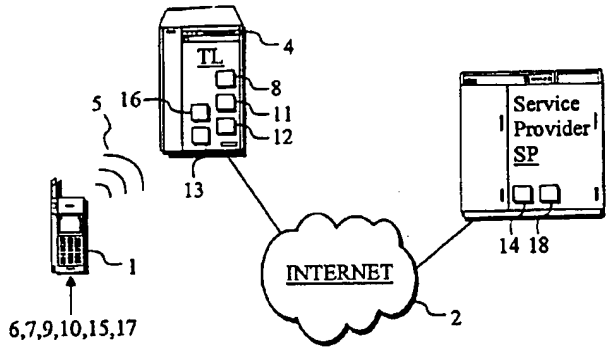
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/GB]; 2 Rushmere Place, Englefield Green, Surrey TW20 0NN (GB).

(74) Agent: PAPULA OY; P.O. Box 981, (Fredrikinkatu 61 A), FIN-00101 Helsinki (FI).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Finnish).

(54) Title: ARRANGEMENT FOR SECURE COMMUNICATION AND KEY DISTRIBUTION IN A TELECOMMUNICATION SYSTEM



(57) Abstract

The present invention relates to telecommunication systems. The object of the invention is to disclose a method and system for secure routing of information and addressing of a service and the parties to the service in a telecommunication system comprising a telecommunication terminal (1); a telecommunication network (2); a service provider (SP) connected to the telecommunication network (2); a service apparatus (4 connected to the telecommunication network (2); and a communication link (5) provided between the telecommunication terminal (1) and the service apparatus (4). In the method, the service apparatus (4) and/or the service mediated by it as well as the telecommunication terminal (1) are provided with an unambiguous identifier associated with predetermined encryption and/or signing keys. Further, a given service apparatus (4) is addressed by means of the telecommunication terminal (1) by sensing a predetermined connection setup request from the telecommunication terminal (1) to the given service apparatus (4). Further, the service provider's (SP) network address and/or other information relating to the selected service is sent from the telecommunication terminal (1) to the service apparatus (4) via the communication link (5). The communication link is preferably based on Bluetooth technology.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Description

Arrangement for secure communication and key distribution in a telecommunication system

FIELD OF THE INVENTION

The present invention relates to telecommunication. In particular, the invention concerns a new type of method and system for secure routing of information and addressing of a service and the parties to a service in a telecommunication system.

BACKGROUND OF THE INVENTION

Mobile stations used in mobile communication networks, e.g. the GSM network (GSM, Global System for Mobile communications), have considerable advantages as compared with wired-network telephones. The greatest advantage is naturally mobility. The use of a mobile station is not dependent on location.

Traditionally, the main purpose of a telephone subscription and the associated terminal equipment is to set up and maintain a speech connection. The use of a mobile station is not limited to the transmission of speech; instead, new functions are continuously being developed for it. Various services based on text messages have become very popular. The popularity of data services is also growing, and it will grow further as the data transmission speed of mobile stations is increased. Third-generation mobile telephones will be capable of real-time transmission of moving images.

A group of leading telecommunication and information technology enterprises have developed a technique which can be used to establish a wireless connection between a mobile station and e.g. a portable computer. This technique is called "Bluetooth" and it is based on short-range radio technology, allowing many types of terminal equipment to be interconnected. A more detailed description of this technique is presented e.g. on WWW page www.bluetooth.com.

The Bluetooth technology allows the interconnection of different devices via a short-range radio link. Using Bluetooth technology, it is possible e.g. to establish a connection between a mobile station and a portable computer without cumbersome cabling. Printers, workstations, telefax devices, keyboards and virtually any digital equipment may form part of a Bluetooth system or network. This technology constitutes a universal bridge to existing data networks and peripherals and it makes it possible to form small private groups via interconnected devices without a fixed network infrastructure. Moreover, encryption and authentication can be used between the devices e.g. so that only a certain user's mobile station may be used in connection with a given portable computer. With Bluetooth, it is possible to use a mobile station for the control of almost any device.

As is known, mobile stations can be used to carry out various purchase or control transactions. A purchase transaction may consist of e.g. the selection of and payment for a product in various automated machines by using a mobile station. The growth of the range of services associated with mobile stations involves a new area. The information to be transmitted is often of a nature that requires that the information be only accessible to the receiver and the sender. It is necessary to provide data security e.g. by employing various encryption methods.

Often the place to which the data regarding a purchase or control transaction needs to be transmitted is not located in the vicinity of the actual place of performance of the purchase or control transaction. There arises the problem of transmitting the information related to the transaction to a central system in a manner as easy and reliable as possible. In addition, at the receiving end it is necessary to be able

to verify an absolute correctness of the information received and to establish the identity of the sender.

At present, the problem is how to address a service party's service apparatus and a given service produced by it. A further problem is how to implement the communication associated with the service transaction and its routing in a secure manner between the parties to the service transaction.

The object of the present invention is to eliminate the drawbacks referred to above or at least to significantly alleviate them.

A specific object of the invention is to disclose a new type of method and system for addressing a service apparatus and a given service associated with it by using a telecommunication terminal, preferably a mobile station. Furthermore, by applying the present invention, a service request can be safely routed to a service provider. The present invention provides a solution for global transmission of remittances from a telecommunication terminal to a payee.

As for the features characteristic of the present invention, reference is made to the claims.

BRIEF DESCRIPTION OF THE INVENTION

The method of the present invention concerns the routing of information and secure addressing of a service and the parties to a service in a telecommunication system. The system comprises a telecommunication terminal, telecommunication network, a service provider connected to the telecommunication network and a service apparatus connected to the telecommunication network. In addition, the system comprises a communication link provided between the telecommunication terminal and the service apparatus.

In the method of the present invention, the telecommunication terminal functions as a selector of a desired service. The telecommunication terminal,

preferably a mobile station, is connected to the service apparatus via the communication link. The communication link may be implemented using Bluetooth technology as described above. This communication link permits the application of required encryption methods to prevent the information transmitted from getting in a useful form into the hands of outsiders. If e.g. Bluetooth technology is employed in the communication link, the connection is assigned during connection setup a one-time identifier for associating the intercommunicating parties with each other. Alternatively, the communication link may consist of e.g. an infrared link. The information to be transmitted can be encrypted by means of the telecommunication terminal, which preferably is a mobile station. In this case, the actual encryption of the information transmitted is performed e.g. by means of a subscriber identity module. The subscriber identity module contains the keys required for encryption and/or signature of the information.

The service apparatus receives the encrypted message from the telecommunication terminal. Part of the message may consist of a service provider's network address determined by the terminal. The network address may also be determined in the service apparatus when it is known which service is meant. Based on the network address, the message is transmitted to the service provider. The network address is preferably an Internet IP address (IP, Internet Protocol). The IP address does not actually define the receiving machine; rather, it defines the connection interface unambiguously in the whole world. It was stated above that the telecommunication network is the Internet. However, this is only one example of possible implementations. The telecommunication network may alternatively be e.g. a bank payment network.

In the method, the telecommunication terminal and/or the service apparatus and/or the service provided by it is assigned an unambiguous identifier. This identifier may be associated with predetermined encryption and/or signing keys. For the encryption of information, the information received from the telecommunication terminal is encrypted and/or signed using the keys associated with the service apparatus and/or service-specific unambiguous identifier, and the encrypted and/or signed information is sent over the telecommunication network to the service provider to a network address determined by the telecommunication terminal or service apparatus. When the service provider receives the encrypted message, the keys needed for its decryption can be determined on the basis of the identifier forming part of the message. In practice, the implementation may be such that the service provider and/or service apparatus communicates with a trusted third party (TTP) e.g. via the telecommunication network. The trusted third party maintains a database containing the encryption and/or signing keys associated with each identifier.

From the trusted third party, the service provider receives information regarding the keys associated with a given identifier, preferably a public encryption and signing key. The service apparatus, too, may communicate with the trusted third party. When the encryption and signature of the message are implemented using a public key method, the authenticity of the message can be reliably verified. On the basis of the identifier, the service apparatus and/or service that the identifier itself is associated with can be determined. The service apparatus may be e.g. a cash machine, a cash system, a computer or an automated service machine.

The encryption of incoming and outgoing messages and the management of the keys, preferably pub-

lic and secret keys, associated with the messages may be implemented using a specific security module. By using such a security module, it is possible to add the use of encryption and message authentication even to equipment in which this feature is originally absent.

The selected service may comprise response and/or control information from the service provider to the service apparatus and/or telecommunication terminal. The service apparatus can be controlled on the basis of a response sent by the service provider. Moreover, information about the progress of the service can be sent to the terminal. An example of this is a case where a telecommunication terminal is used e.g. as a means of payment. A service request is sent from the terminal to the service provider and the service provider informs the terminal about success or failure of the service. Payment arrangements may additionally comprise a feature requiring that the payment transaction be separately confirmed. Confirmation is accomplished e.g. by having the telecommunication terminal send a service-specific confirmation code in a separate message to the service provider. Separate message here means e.g. an encrypted SMS message (SMS, Short Message Service). Having interpreted the SMS message received, the service provider sends to the service apparatus a permission to carry out the service.

An example of the protocol to be used between the telecommunication terminal and the service provider is the WAP (Wireless Application Protocol). The WAP protocol defines a standard for applications providing services to terminals in a wireless network. Using the WAP protocol, it is possible e.g. to establish a telephone connection to a WWW server. In addition, e.g. the WML language (Wireless Markup Language), which is the description language of the WAP protocol, is used in conjunction with a WAP implemen-

tation. WML is a description language resembling the HTML language (HTML, HyperText Markup Language), adapted for a wireless environment.

The system of the present invention comprises means for providing a telecommunication terminal with an unambiguous terminal-specific identifier, means for addressing a given service apparatus by means of a telecommunication terminal by sending from the telecommunication terminal a predetermined connection setup request to the given service apparatus, means for providing the service apparatus and/or the service mediated by it with an unambiguous service-specific identifier, said identifier being associated with predetermined encryption and/or signing keys, and means for sending the service provider's network address and other information relating to the selected service from the telecommunication terminal to the service apparatus via a communication link.

The system further comprises means for addressing a given service apparatus by means of a telecommunication terminal by sending from the telecommunication terminal a predetermined connection setup request to a given service apparatus via a communication link. In addition, the system comprises means for encrypting and/or signing the information received from the telecommunication terminal using keys associated with the service-specific and/or service apparatus-specific identifier and means for sending encrypted and/or signed information via the telecommunication network to the service provider to a network address determined by the telecommunication terminal and/or service apparatus.

The system of the present invention comprises means for controlling the service apparatus on the basis of information sent by the service provider and means for sending confirmation and/or other information from the service provider to the service appara-

tus and/or to the telecommunication terminal. The system further comprises means for sending a message confirming the service transaction from the telecommunication terminal to the service provider if a predetermined condition is fulfilled and means for accepting the required service request only when the service apparatus receives from the service provider a confirmation code confirming the service transaction. In addition, the system comprises means for encrypting the communication.

The system of the present invention comprises a trusted third party which communicates with the service apparatus and/or service provider over the telecommunication network. Further, the service provider and/or service apparatus comprises means for sending to the trusted third party an inquiry regarding the encryption and/or signing keys associated with each unambiguous identifier.

The present invention has many advantages. By applying the invention, it is possible to address a given service apparatus associated with a service, a given service mediated by it and a given telecommunication terminal. Furthermore, the invention makes it possible to individuate the service provider associated with a selected service and to send to the service provider encrypted information relating to the service. For the user, a significant advantage is the low cost of the services. As the method does not necessarily require the setup of a connection chargeable by the operator, the cost of the service to the user is low. An additional reason for the low cost is that the communication between the service apparatus and the service provider takes place in an existing data network, e.g. the Internet.

LIST OF ILLUSTRATIONS

In the following, the invention will be de-

scribed in detail by the aid of a few examples of its embodiments, wherein

Fig. 1 presents a preferred system according to the invention, and

Fig. 2 presents a flow diagram representing the operation of a preferred example of the system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A system as presented in Fig. 1 comprises a telecommunication terminal, a service apparatus 4 and a service provider SP. The telecommunication terminal 1 is connected via a communication link 5 to the service apparatus 4. The telecommunication terminal 1 is preferably a mobile station. The communication link 5 may be e.g. a connection based on Bluetooth technology. The service apparatus 4 and the service provider SP are connected to a telecommunication network 2. The telecommunication network 2 is preferably the global Internet network. Alternatively, the telecommunication network 2 may be e.g. a bank payment network. Use of the Internet has the advantage that the network covers a very large area and that the devices attached to it can be unambiguously identified.

The receiver of a service request is indicated using a network address which is set by means of the telecommunication terminal 1 or the service apparatus 4; in this example, the address is an IP address. By virtue of the IP address, the receiver of the service request being sent is unambiguously defined.

The service provider SP identifies the sending service apparatus 4 by a globally unambiguous identifier included in the message. The identifier individuates the message decryption keys associated with the identifier. In addition, based on the identifier, the service provider SP is able to send the service

apparatus 4 a response to the service request if necessary. For each service apparatus-specific identifier, the service provider SP knows an unambiguous network address.

The telecommunication terminal 1 comprises means 6 for providing it with a terminal-specific unambiguous identifier and means 7 for addressing a given service apparatus by sending from the terminal 1 a predetermined connection setup request to the service apparatus 4. Using means 9, the service provider's network address and/or other information relating to the service is sent to the service apparatus 4 via the communication link 5. Using means 10, a given service apparatus 4 is addressed via the communication link 5. Moreover, the telecommunication terminal 1 comprises means 15 for sending a confirmation message confirming the service transaction to the service provider SP. Using means 17, the communication 5 can be encrypted.

The service apparatus 4 comprises means 8 for providing the service apparatus and/or the service mediated by it with an unambiguous identifier, said identifier being associated with predetermined encryption and/or signing keys. Using means 11, the information received from the telecommunication terminal 1 is encrypted using the keys associated with the service-specific and/or service apparatus-specific identifier. Further, using means 12, the encrypted information is sent via the telecommunication network 2 to the service provider. The service apparatus 4 additionally comprises means 13 for controlling the service apparatus 4 on the basis of information sent by the service provider SP. Using means 16, the required service is only accepted when the service apparatus 4 receives from the service provider SP a confirmation code for the service transaction.

The service provider SP comprises means 14 for sending confirmation and/or other information to

the service apparatus 4 and/or to the telecommunication terminal 1. Using means 18, a query asking for the encryption and/or signing keys associated with each unambiguous identifier is sent to a trusted third party.

Fig. 2 presents a preferred example of a flow diagram showing the steps comprised in a service according to the invention. The client establishes a communication connection to a service apparatus of his selection, block 20. The communication connection between the terminal and the service apparatus is established e.g. via a Bluetooth link. As indicated in block 21, the client selects a desired service and the associated parameters by means of his terminal. The service is e.g. payment of a bill at the cash desk of a store. A service request is sent via the communication link to the service apparatus, block 22. A communication connection using Bluetooth technology includes encryption of the communication. After all the information required for the service has been received from the telecommunication terminal, the operations required by the service itself are carried out, block 23.

For the service apparatus and/or the service produced by it, an unambiguous identifier linking a given service apparatus and the associated encryption keys together has been defined beforehand. Based on this identifier, the service provider knows where the message received comes from. The telecommunication terminal or the service apparatus adds the required network address to the message to be sent. The service apparatus encrypts the message and sends it to the service provider over a telecommunication network. In this example, the telecommunication network is a bank payment network.

Using the decryption keys associated with the identifier, the service provider decrypts the received

message. To ensure an effective management of the keys, the database consisting of the identifiers and the associated decryption keys is maintained e.g. by a trusted third party. If the service request concerns a payment at a cash desk as in the above example, then in this case the service provider may be a bank. Depending on the service, a decision is made whether a confirmation of execution of the service is to be sent or not, block 24. The service provider may send to the service apparatus or telecommunication terminal an encrypted response to the service request, blocks 26 and 27. The service may also be of a nature that requires no response, block 25. The service provider encrypts the message with his own secret signing key and finally encrypts the entire message using a public encryption key associated with the service apparatus. The service apparatus has the required decryption keys for the deciphering of the message. As indicated in block 29, a confirmation for the execution of the service transaction can also be sent to the telecommunication terminal. According to the above description, the message sent may consist of information indicating that the bill was successfully paid. A confirmation of execution of the service need not necessarily be sent to the telecommunication terminal, block 28.

In an embodiment as illustrated in Fig. 1, the service in question is a cash service. Each cash register terminal in the store is provided with communication equipment consistent with the Bluetooth technology. Further, the terminal equipment of the client using the cash service has the readiness for Bluetooth communication. In this example, the client's terminal is a mobile station. The client wants to pay for his shopping by using a Bluetooth interface. Since the maximum range of a Bluetooth connection varies from ten meters to a few tens of meters depending on the case, there may be several cash register terminals

within that area which are capable of receiving radio signals. Therefore, the client needs to individuate the cash register terminal with which a connection is to be established. The Bluetooth technology includes encryption of radio communication, so information can be securely transferred via the wireless link. The mobile station individuates the selected cash register terminal e.g. by sending a signal containing the number of the cash register terminal. The connection is assigned a temporary identifier by which the communicating parties identify each other. Alternatively, the mobile station contains e.g. an electronic component which is identified by the cash register terminal when the mobile station is moved at a sufficiently short distance from the cash register terminal.

Via the Bluetooth link, the cash register terminal sends the information it has received about the service to the service provider. The service provider in this example is a bank. The service information includes e.g. the account to be charged, service provider address data, the sum to be charged and other possible information relevant to the particular service. The service provider is individuated by means of a given predetermined network address. This address is included in the information provided in the mobile station prior to the service transaction. Alternatively, the network address may be determined by the cash register terminal. The information transmitted between the cash register terminal and the service provider is encrypted to prevent misuse. The information is encrypted using encryption keys specific to the service apparatus and/or service. The service provider possesses the keys required for the decryption of the information transmitted.

The user of the service has to confirm the service request if the amount to be paid exceeds a certain limit, e.g. $ 50. For the confirmation, the

service provider sends via the cash register terminal to the mobile station a confirmation reference, which the mobile station has to return to the service provider e.g. in an SMS message. The user includes the confirmation code in the message, encrypts and/or signs the message and sends the encrypted message to the service provider. The service provider decrypts the message and thus verifies the identity of the user and interprets the information contained in the message. The service provider sends the user a message indicating successful remittance of the payment e.g. over the Bluetooth link via the cash register terminal.

In an embodiment as illustrated in Fig. 1, the method of the invention is applied in an automatic gas station in conjunction with refueling. The client wants to fill the fuel tank of a company car. The company car has been fitted with a Bluetooth communication device. When the car arrives at the filling place, the communication device sets up a radio connection with the automatic filling machine. The communication device in the car contains information including the account of the company, the network address of the service provider (bank) and other possible information. The client confirms the payment transaction using a predetermined identifier. This ensures that a person illicitly using the car will not be able to refuel the car on the company's account. The communication between the automatic filling machine and the service provider is encrypted using an encryption key associated with the filling machine. The service provider transmits a response message to the filling machine, which sends it further to the communication device in the client's company car.

The invention is not restricted to the examples of its embodiments described above; instead, many

variations are possible within the scope of the inventive idea defined in the claims.

Claims

CLAIMS

1. Method for secure routing of information and addressing of a service and the parties to the service in a telecommunication system comprising

a telecommunication terminal (1),

a telecommunication network (2),

a service provider (SP) connected to the telecommunication network (2),

a service apparatus (4) connected to the telecommunication network (2),

a communication link (5) provided between the telecommunication terminal (1) and the service apparatus (4),

characterized in that the method comprises the steps of:

providing the telecommunication terminal (1) with a terminal-specific unambiguous identifier;

addressing a given service apparatus (4) by means of the telecommunication terminal (1) by sending a predetermined connection setup request from the terminal (1) to the given service apparatus (4);

providing the service apparatus (4) and/or the service mediated by it with a service-specific unambiguous identifier, said identifier being associated with predetermined encryption and/or signing keys; and

sending the service provider's (SP) network address and/or other information relating to the selected service from the telecommunication terminal (1) to the service apparatus (4) via the communication link (5).

2. Method as defined in claim 1, characterized in that the given service apparatus (4) is addressed by means of the telecommunication terminal (1) by sending from the telecommunication terminal (1) a predetermined connection setup request to the given service apparatus (4) via the communication link (5).

3. Method as defined in claim 1 or 2, characterized in that

the information received from the telecommunication terminal (1) is encrypted and/or signed by using the keys associated with the service-specific and/or service apparatus-specific identifier; and

the encrypted and/or signed information is sent over the telecommunication network (2) to the service provider (SP) to an address determined by the telecommunication terminal (1).

4. Method as defined in any one of the preceding claims 1 - 3, characterized in that the service apparatus (4) is controlled on the basis of information sent by the service provider (SP).

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that confirmation and/or other information is sent from the service provider (SP) to the service apparatus (4) and/or to the telecommunication terminal (1).

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that a message confirming the service transaction is sent by the telecommunication terminal (1) to the service provider (SP) if a predetermined condition is fulfilled.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that a message confirming the service transaction is sent by the telecommunication terminal (1) to the service provider (SP) in the form of an SMS message.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that the service request is only accepted after the service apparatus (4) has received from the service provider (SP) a confirmation code for the service transaction.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that

the communication connection (5) is a link based on Bluetooth technology.

10. Method as defined in any one of the preceding claims 1 - 9, characterized in that the communication connection (5) is an infrared link.

11. Method as defined in any one of the preceding claims 1 - 10, characterized in that the communication connection (5) is encrypted.

12. Method as defined in any one of the preceding claims 1 - 11, characterized in that a public key and/or private key encryption and/or signing method is applied.

13. Method as defined in any one of the preceding claims 1 - 12, characterized in that the WAP is used between the telecommunication terminal (1) and the service apparatus (4) and/or the service provider (SP).

14. Method as defined in any one of the preceding claims 1 - 13, characterized in that the service provider communicates with a trusted third party, which third party maintains a database which containing the encryption and/or signing keys associated with each identifier.

15. Method as defined in any one of the preceding claims 1 - 14, characterized in that the service provider (SP) and/or the service apparatus (4) sends to the trusted third party an inquiry asking for the encryption and/or signing keys associated with each unambiguous identifier.

16. Method as defined in any one of the preceding claims 1 - 15, characterized in that the network address is an IP address.

17. System for secure routing of information and addressing of a service and the parties to the service in a telecommunication system comprising

a telecommunication terminal (1),

a telecommunication network (2),

a service provider (SP) connected to the telecommunication network (2),

a service apparatus (4) connected to the telecommunication network (2),

a communication link (5) provided between the telecommunication terminal (1) and the service apparatus (4),

characterized in that the system comprises:

means (6) for providing the telecommunication terminal (1) with a terminal-specific unambiguous identifier;

means (7) for addressing a given service apparatus (4) by means of the telecommunication terminal (1) by sending a predetermined connection setup request from the terminal (1) to the given service apparatus (4);

means (8) for providing the service apparatus (4) and/or the service mediated by it with a service-specific unambiguous identifier, said identifier being associated with predetermined encryption and/or signing keys; and

means (9) for sending the service provider's (5) network address and/or other information relating to the selected service from the telecommunication terminal (1) to the service apparatus (4) via the communication link (5).

18. System as defined in claim 17, characterized in that the system comprises means (10) for addressing a given service apparatus (4) using the telecommunication terminal (1) by sending from the telecommunication terminal (1) a predetermined connection setup request to the given service apparatus (4) via the communication link (5).

19. System as defined in claim 17 or 18, characterized in that the system comprises

means (11) for encrypting and/or signing the information received from the telecommunication terminal

(1) using the keys associated with the service-specific and/or service apparatus-specific identifier; and

means (12) for sending the encrypted and/or signed information over the telecommunication network (2) to the service provider (SP) to a network address determined by the telecommunication terminal (1) and/or the service apparatus (4).

20. System as defined in any one of the preceding claims 17 - 19, characterized in that the system comprises means (13) for controlling the service apparatus (4) on the basis of information sent by the service provider (SP).

21. System as defined in any one of the preceding claims 17 - 20, characterized in that the system comprises means (14) for sending confirmation and/or other information from the service provider (SP) to the service apparatus (4) and/or to the telecommunication terminal (1).

22. System as defined in any one of the preceding claims 17 - 21, characterized in that the system comprises means (15) for sending a message confirming the service transaction from the telecommunication terminal (1) to the service provider (SP) if a predetermined condition is fulfilled.

23. System as defined in any one of the preceding claims 17 - 22, characterized in that the system comprises means (16) for only accepting a service request after the service apparatus (4) has received from the service provider (SP) a confirmation code for the service transaction.

24. System as defined in any one of the preceding claims 17 - 23, characterized in that the system comprises means (17) for encrypting the communication connection (5).

25. System as defined in any one of the preceding claims 17 - 24, characterized in

that the system comprises a trusted third party which communicates with the service apparatus (4) and/or the service provider (SP) over the telecommunication network (2).

26. System as defined in any one of the preceding claims 17 - 25, characterized in that the service provider (SP) and/or the service apparatus (4) comprises means (18) for sending to the trusted third party an inquiry asking for the encryption and/or signing keys associated with each unambiguous identifier.

27. System as defined in any one of the preceding claims 17 - 26, characterized in that the telecommunication terminal (1) is a mobile station with a subscriber identity module connected to it.

28. System as defined in any one of the preceding claims 17 - 27, characterized in that the service apparatus (4) is an automatic teller machine.

29. System as defined in any one of the preceding claims 17 - 27, characterized in that the service apparatus (4) is a cash register system.

30. System as defined in any one of the preceding claims 17 - 27, characterized in that the service apparatus (4) is a computer.

31. System as defined in any one of the preceding claims 17 - 27, characterized in that the service apparatus (4) is an automated service machine, e.g. an automatic gasoline filling machine.

32. System as defined in any one of the preceding claims 17 - 31, characterized in that the telecommunication network (2) is the Internet network.

33. System as defined in any one of the preceding claims 17 - 31, characterized in

that the telecommunication network (2) is a bank payment network.

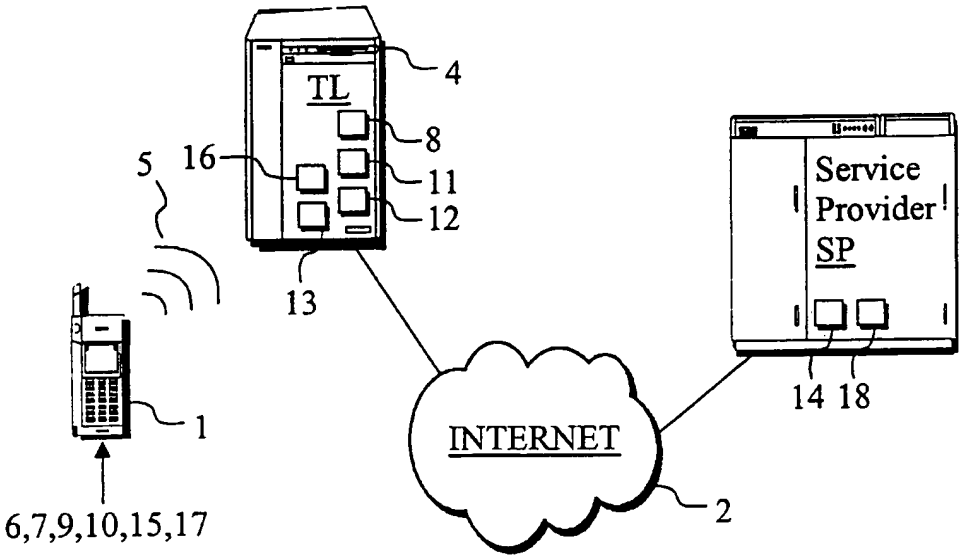

TL
4
8
11
12
5
16
13
Service
Provider
SP
14 18
INTERNET
2
1
6,7,9,10,15,17

Fig. 1

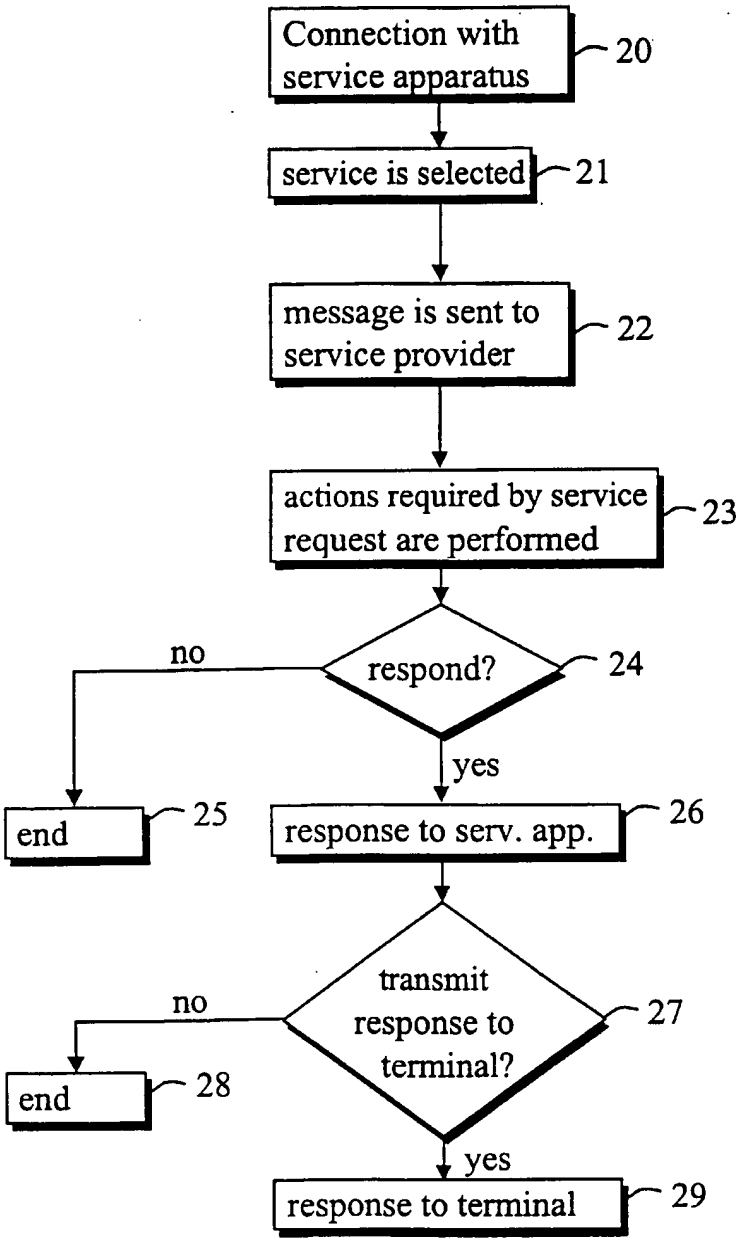

Connection with service apparatus
20
service is selected
21
message is sent to service provider
22
actions required by service request are performed
23
respond?
24
no
yes
end
25
response to serv. app.
26
transmit response to terminal?
27
no
end
28
yes
response to terminal
29

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00223

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 9/08
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Ericsson Review, Volume, No 3, 1998, JAAP HAARTSEN, "Bluetooth - The universal radio interface for ad hoc, wireless connectivity", see the whole document ---	1-33
Y	WO 99/00958 A1 (BRITISH TELECOMMUNICATIONS PLC), 7 January 1999 (07.01.99), page 3, line 15 - line 28, abstract --- --------	1-33

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 August 2000	11 -08- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer THOMAS THOLIN/EE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI 00/00223

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 99/00958 A1	07/01/99	NONE	